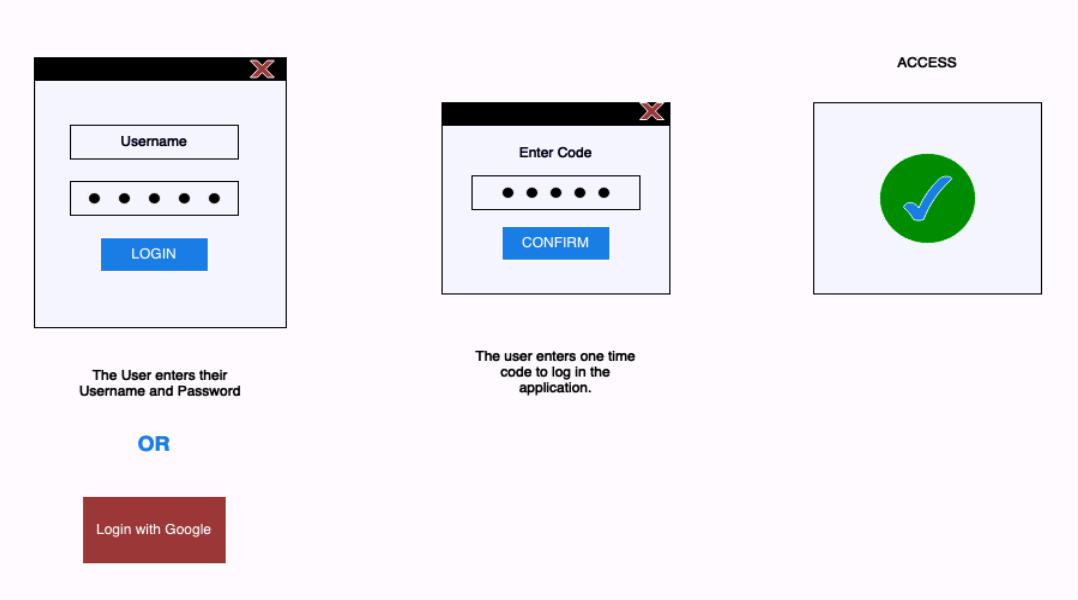
Strong Authentication - MFA

Introduction:

In the past when a user wanted to transfer money online, he had to log in to that bank's web application via his username and password. With impressive technological advancements, cyber crimes have increased as well. Hence, this username and password can be stolen by anyone. So in order to assure that the user who is attempting to log in using the username and password is actually the user, the bank's website uses Multi Factor Authentication(MFA). If this web site has been configured to perform MFA, the user who tries to log in to the web application has to give the username and password along with an additional authentication step, such as one-time password(OTP), sent to the user's mobile number. Hence, this transaction is safer than using only the username and password.

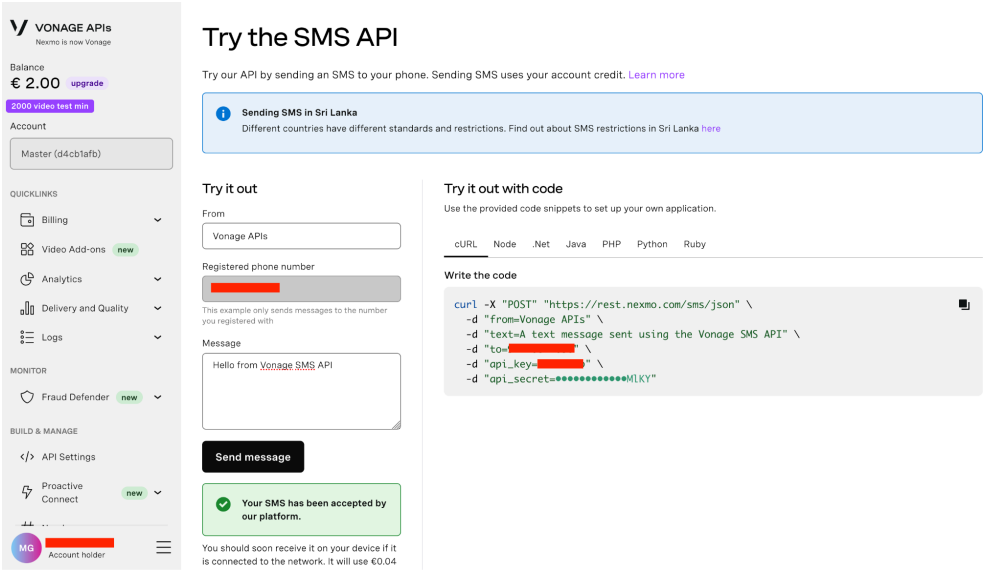
To demonstrate this scenario, we are going to log in to a sample web application called pickup-dispatch using MFA. In the first step the user has to provide their username/password. Once he is authenticated, the user receives a one-time password to their registered mobile phone.



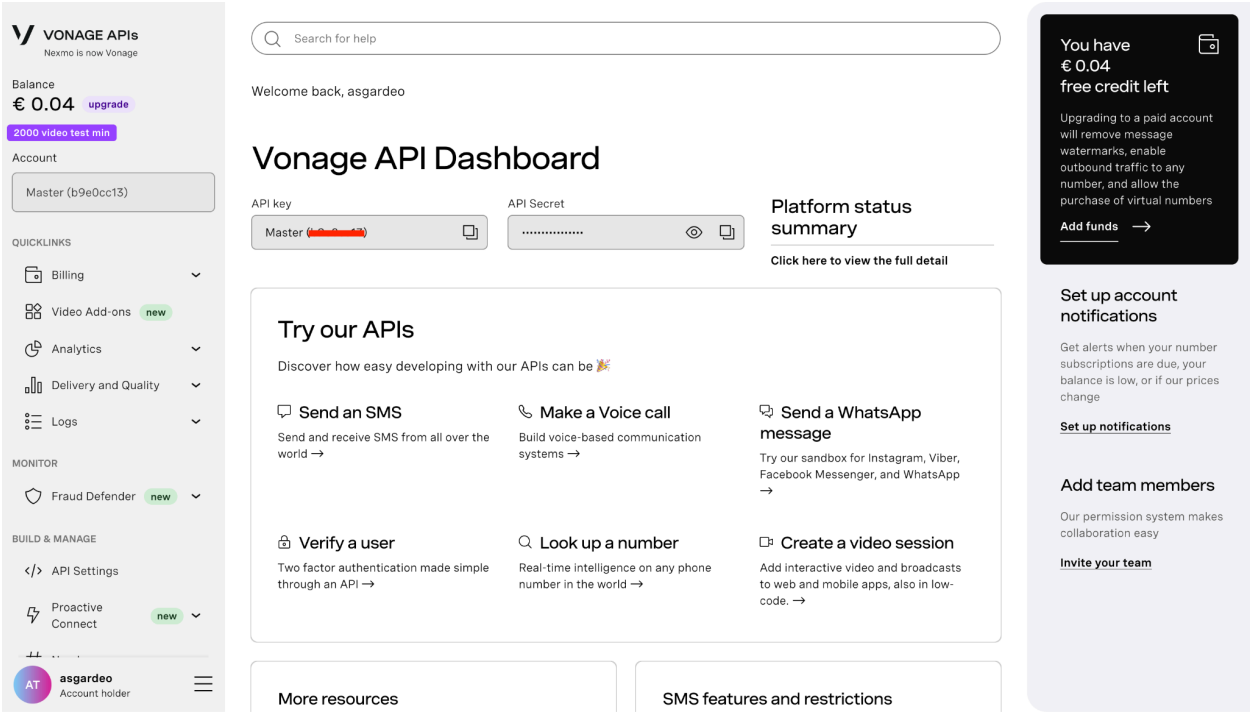
Setting up:

Create a Nexmo Service Provider application to configure OTP

1. Go to https://dashboard.nexmo.com/sign-up and sign up and start working with **SMS**.
    a. This will create an API **key** and a **secret** for you.
2. Once the sign up is done, test it by clicking on **Send message**.

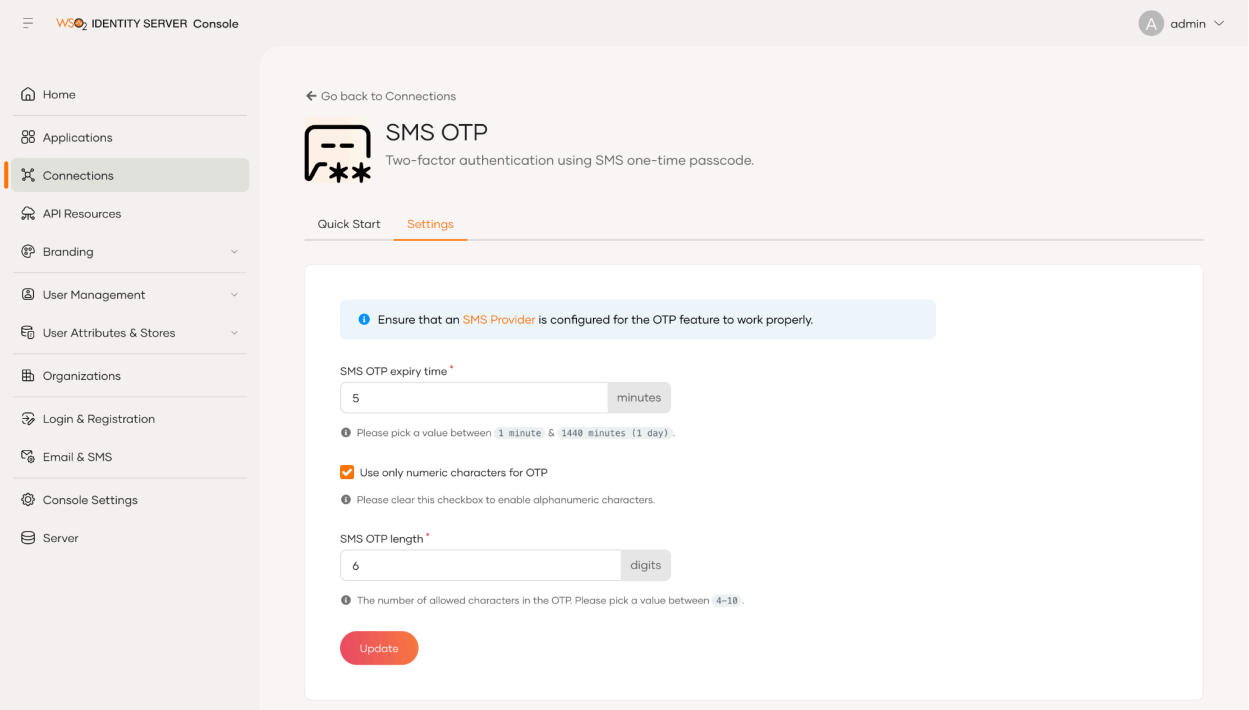


3. Goto the home screen using https://dashboard.nexmo.com/ and the **API Key** and **Secret** are displayed in. Copy and save them as you need them for the next step.



Configure SMS OTP

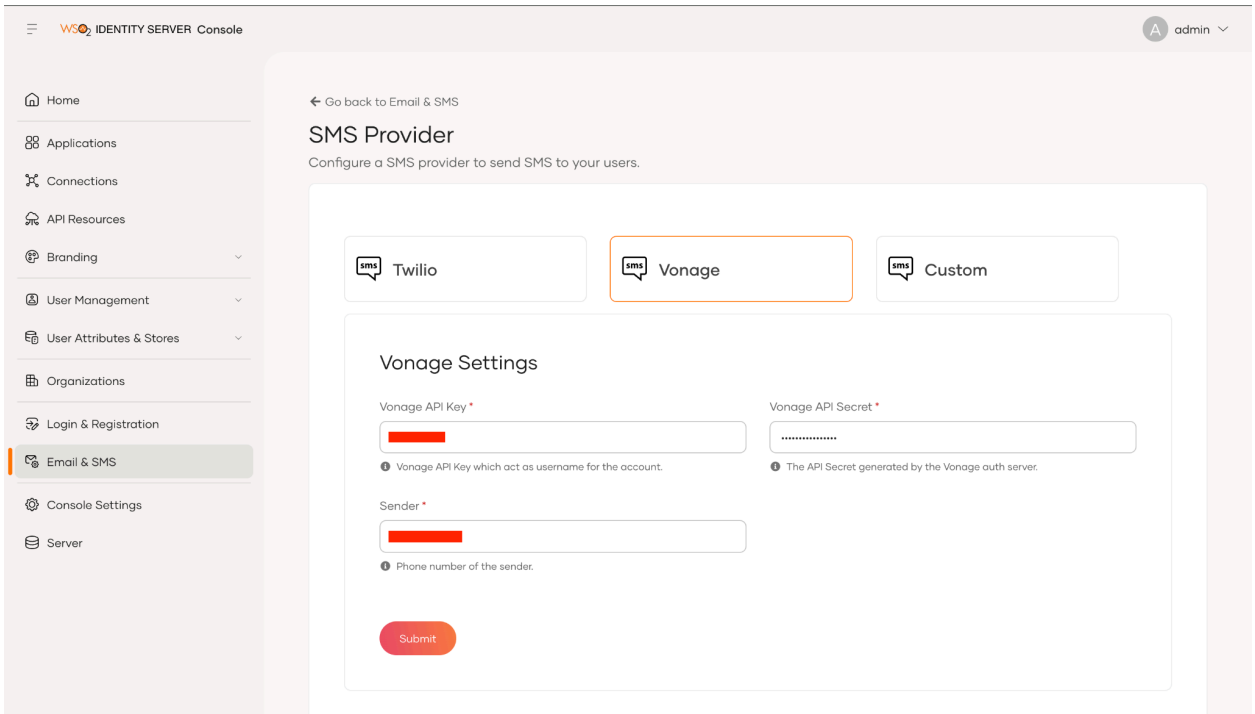
1. Login to the WSO2 Identity Server **Console,** using your admin credentials (e.g. admin:admin).
2. In the WSO2 Identity Server **Console,** from the menu click **Connections.**
3. Open the **SMS OTP** local authenticator listed.
4. You will be prompted to the below page.



5. For the simplicity of this tutorial, let's keep the default configuration.
6. Create SMS Provider,
    a. In the WSO2 Identity Server **Console,** from the menu click **Email & SMS.**
    b. Select **SMS Provider**.
    c. To create a Vonage SMS Provider click on the **Vonage** option.

d. Paste the API **Key** and **Secret** you saved in Create a Nexmo Service Provider step.

e. Enter the phone number you provided to Nexmo in the **Sender** field.

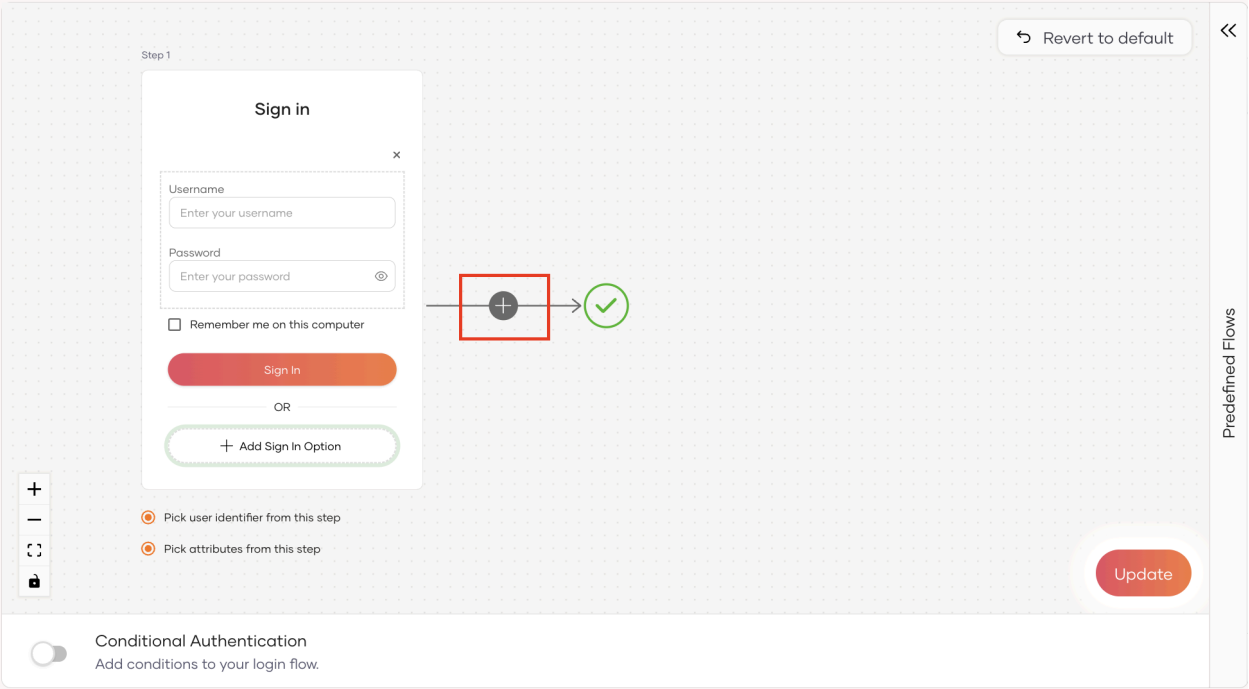


f. Click **Submit**.

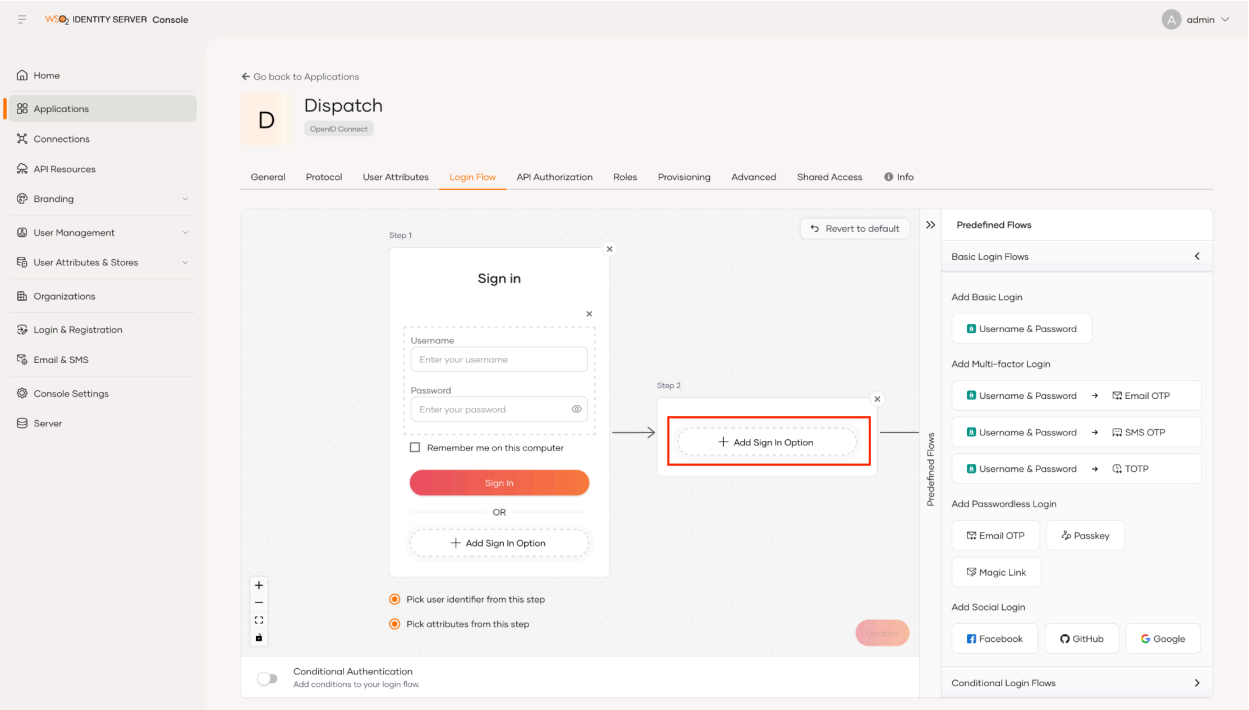
Configure MFA to the sample application

Let's SMS OTP as the 2nd factor of authentication.

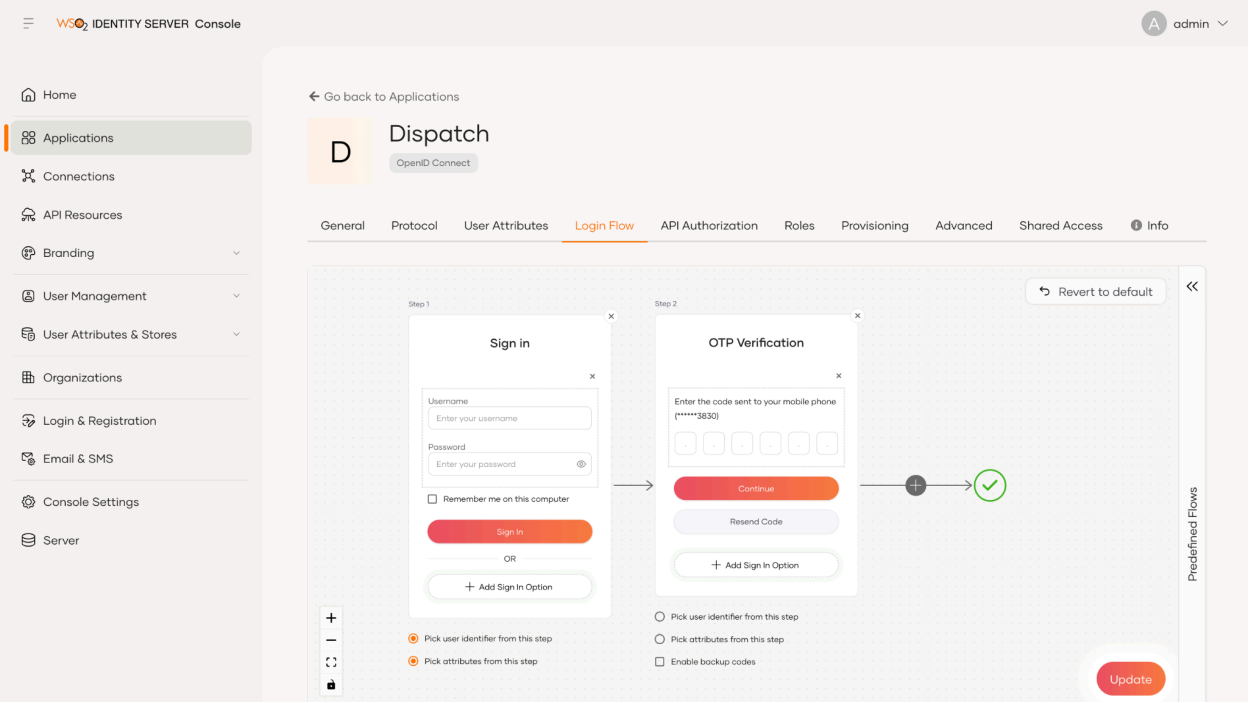
1. Use the **Dispatch** Application configured in **5. Single Sign-On with OpenID Connect** Lab.
2. In the WSO2 Identity Server **Console,** from the menu click **Applications.**
3. Click on application **Dispatch.**
4. Goto the **Login Flow**.
5. Click on **Revert to default**, to remove previously configured authentication mechanisms.
6. Next select **+** icon followed by the screen.



7. Click on the **+ Add Sign In Option** of the 2nd step.



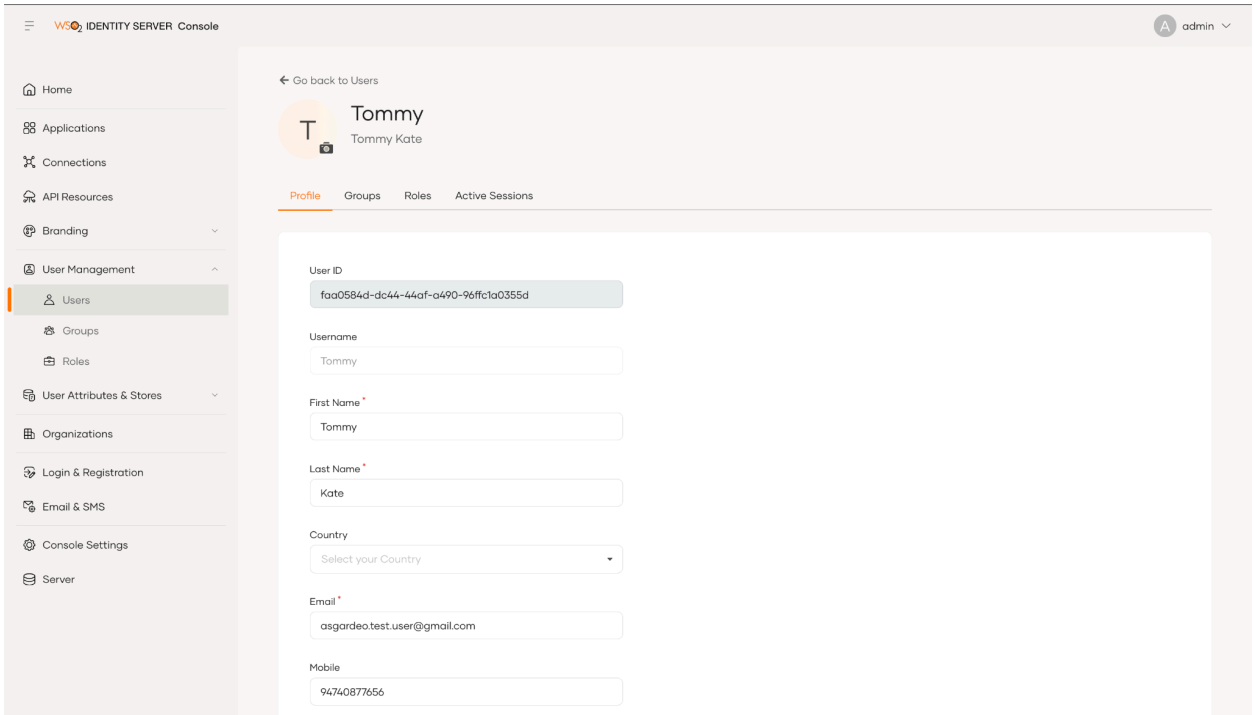
8. From the listed authentication methods, select **SMS OTP**.



9. Click **Update**.

Update the user

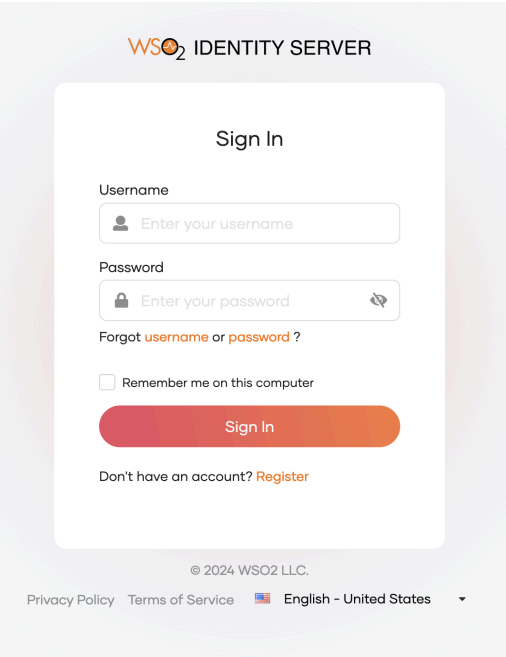
1. In the WSO2 Identity Server **Console,** from the menu click **User Management.**
2. Select User.
3. From the list of users, select the user **Tommy.**
4. Add a **Mobile Number** to the respective fields.



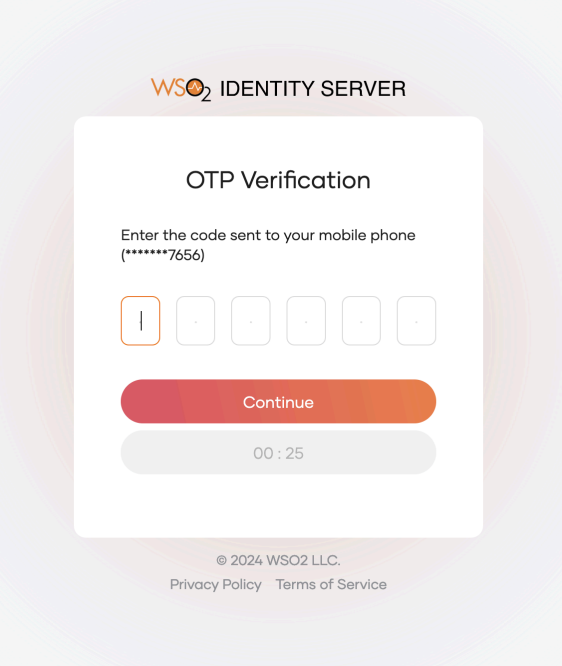
5. Click Update.

Try It:

1. Go to http://localhost.com:8080/pickup-dispatch and click on the login button.
2. You will be redirected to the login page of WSO2 Identity Server. This login page consists of an option to enter the username and password. Type credentials of **Tommy**.



3. Once the above step is successful, you will be redirected to a page where you have to enter the one-time password(OTP) that has been sent to the mobile number configured in your profile.



4. Once you enter a valid OTP, you will be able to log in to the pickup-dispatch application. If you do not enter the OTP, you will not be able to log into the application due to an authentication failure.